# UNITED STATES DISTRICT COURT

for the

Central District of California

| | | |
|---|---|---|
| In the Matter of the Search of<br>Red iPhone, currently in the custody of the Drug Enforcement Administration, in Los Angeles, California, as further described in Attachment A | ) | Case No. 2:23-MJ-3629 |

**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property

*See Attachment A*

located in the Central District of California, there is now concealed:

*See Attachment B*

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| | |
|---|---|
| 21 U.S.C. § 841(a)(1) | Distribution of controlled substance with intent to distribute |
| 21 U.S.C. § 846 | Conspiracy to distribute controlled substance |

The application is based on these facts:

*See attached Affidavit*

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*/s/*

*Applicant's signature*

Andrea Ferdinand, Special Agent, DEA

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

*Judge's signature*

City and state: Los Angeles, CA

Hon Rozella A. Oliver, United States Magistrate Judge

*Printed name and title*

AUSA: Jeremy K. Beecher (213) 894-5429

# AFFIDAVIT

I, Andrea Ferdinand, being duly sworn, declare and state as follows:

## I. INTRODUCTION

1. I am a Special Agent ("SA") with the Drug Enforcement Administration ("DEA") and have been so employed since May 2017. I am currently assigned to the Los Angeles Field Division ("LAFD"), Enforcement Group 5 ("Group 5") Los Angeles, California, Group 5, an enforcement group investigating narcotics trafficking and money laundering violations under Titles 18 and 21 of the United States Code. I have received 19 weeks of specialized training in Quantico, Virginia, pertaining to narcotics trafficking, money laundering, undercover operations, and electronic and physical surveillance procedures. I have been involved in numerous investigations dealing with the possession, manufacturing, distribution, and importation of controlled substances as a SA with DEA. Based on my training and experience, I am familiar with narcotics traffickers' methods of operation including the distribution, storage, and transportation of narcotics and the collection of money proceeds of narcotics trafficking. I am also familiar with methods employed by large narcotics organizations to thwart detection by law enforcement, including the use of debit calling cards, public telephones, cellular telephone technology, beepers, counter surveillance, false or fictitious identities, and encoded communications.

2. I have also assisted in investigations into the unlawful importation, possession with intent to distribute, and distribution of controlled substances, as well as the related laundering of monetary instruments and the conducting of monetary transactions involving the proceeds of specified unlawful activities and conspiracies associated with criminal narcotics and money laundering offenses.

3. To successfully conduct these investigations, I have utilized a variety of investigative techniques and resources, including physical and electronic surveillance and the use of various types of informants and cooperating sources. Through my training, experience, and continued interaction with experienced special agents, task force officers ("TFO"), and other investigators, I have become familiar with methods employed by narcotic traffickers in general, to smuggle, safeguard, and distribute narcotics, and to collect and launder narcotic-related proceeds. Further, I have been the affiant for and have assisted in numerous drug trafficking investigations in which cellular telephone communications played a major role in the communication network of drug trafficking organizations.

## II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application for a warrant to search one red iPhone cell phone, using phone number 562-665-1161, Device ID 891480000072656697 35 (the "SUBJECT DEVICE")

seized from and belonging to Juan Carlos GUTIERREZ ("GUTIERREZ") and currently in the custody of the Drug Enforcement Administration, in Los Angeles, California, as described more fully in Attachment A.

5. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of the violation of 21 U.S.C. § 841(a)(1) (distribution and possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute and possess with intent to distribute controlled substances) (the "SUBJECT OFFENSES"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## III. STATEMENT OF PROBABLE CAUSE

7. Based on my review of DEA and Long Beach Police Department ("LBPD") law enforcement reports of the incidents below, my

conversations with other law enforcement officers, and my personal involvement in the investigation, I know the following:

**A. The Grand Jury Charges GUTIERREZ by Indictment for Distribution of Fentanyl Causing the Death of S.R.**

8. On December 10, 2021, a 34-year-old male, victim S.R., was found dead inside his residence at a drug rehabilitation home run by Safe Refuge Rehabilitation in Long Beach. The Los Angeles County Coroner's Office subsequently ruled S.R.'s cause of death as "fentanyl toxicity."

9. On April 25, 2023, the grand jury in this District charged GUTIERREZ by indictment in United States v. Juan Carlos Gutierrez, Case Number 2:23-cr-197-SB, for knowingly and intentionally distributing fentanyl, the use of which resulted in victim S.R.'s death, in violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(C). The same day, the Hon. Alicia G. Rosenberg, United States Magistrate Judge, issued a warrant for GUTIERREZ's arrest on the charge in the indictment.

**B. DEA Arrests GUTIERREZ and Seizes the SUBJECT DEVICE**

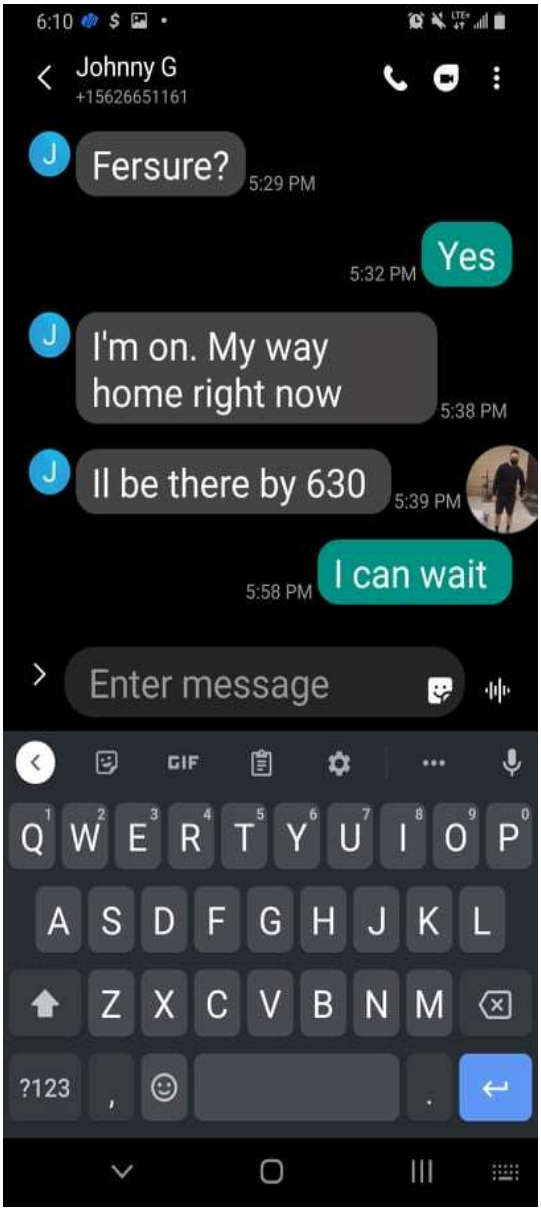
10. On May 2, 2023, DEA agents executed the federal arrest warrant for GUTIERREZ at his residence in Montebello, California. In a search of GUTIERREZ's person incident to the arrest, DEA agents seized the SUBJECT DEVICE and a small bag of a white substance from

GUTIERREZ's pocket that subsequently tested positive for fentanyl. GUTIERREZ did not provide consent to search the SUBJECT DEVICE.

**C. Use of the SUBJECT DEVICE in the SUBJECT OFFENSES**

11. During the fentanyl transaction that led to S.R.'s death, GUTIERREZ used the SUBJECT DEVICE, the phone number of which is 562-665-1161, to communicate with co-conspirator Jayleen Feusier, who obtained the fentanyl from GUTIERREZ and delivered it to S.R., thus

causing his death. For instance, a review of S.R.'s phone pursuant to a state-issued search warrant showed that while facilitating the delivery of fentanyl to S.R. on December 9, 2021, Feusier told S.R. that her dealer was ten minutes away. Feusier sent to S.R. as corroboration the following image, a screen-shot of text messages between Feusier and GUTIERREZ which displayed GUTIERREZ's cell phone number, which is linked to the SUBJECT DEVICE:



12. Feusier's subsequent texts with S.R. indicate that she then obtained fentanyl from GUTIERREZ at GUTIERREZ's residence, likely necessitating further communications between the two.

13. On April 11, 2023, the Hon. Pedro V. Castillo, United States Magistrate Judge, issued a warrant authorizing the search of Feusier's cell phone. (Case No. 2:23-MJ-01728.) An analysis of the contents of Feusier's cell phone showed multiple narcotics-related text message threads between Feusier and GUTIERREZ using the phone number linked to the SUBJECT DEVICE, including conversations in which Feusier sought to obtain fentanyl from GUTIERREZ. In addition, GUTIERREZ's phone number was listed as a saved contact on Feusier's phone. There also were multiple CashApp transactions between GUTIERREZ and Feusier which, in the context of the narcotics-related text message threads between them, appear to represent payment for narcotics.

14. Based on my training, experience and knowledge of this case, I believe the SUBJECT DEVICE will contain the following: evidence of narcotics trafficking including, but not limited to, evidence regarding the coordination of the narcotics transaction on December 9, 2021, between GUTIERREZ and Feusier during which Feusier purchased the fentanyl that caused S.R.'s fatal overdose; evidence that GUTIERREZ sourced Feusier with fentanyl upon this and several other occasions; evidence coinciding with intelligence that

investigators have collected regarding this investigation and solidify what is believed to be GUTIERREZ's role as the supplier of the fentanyl that caused S.R.'s fatal overdose; and evidence establishing GUTIERREZ's knowledge of the particular type of narcotics (i.e. fentanyl) that he distributed to Feusier. I further believe the SUBJECT DEVICE may contain evidence that will help investigators identify GUTIERREZ's source for obtaining fentanyl.

## IV. TRAINING AND EXPERIENCE ON DRUG OFFENSES

15. Based on my training and experience and familiarity with drug trafficking investigations by other law enforcement agents, I know the following:

a. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. These records are often maintained where the drug trafficker has ready access to them, such as on his or her cell phone(s) and other digital devices.

b. Communications between people buying and selling drugs often take place by telephone calls and digital media, including e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. Such communications between the seller and the buyer include sending photos or videos of the drugs, price negotiation

price, and discussions of whether participants will bring weapons to a deal. In addition, drug traffickers' photos and videos on their digital devices often depict the drugs in their possession, and they frequently send these photos and videos among themselves or to others to boast about the drugs or to advertise drug sales.

c. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices, as well as records of meetings with associates, customers, and suppliers, including in the form of calendar entries and location data.

d. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

## V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

16. As used herein, the term "digital device" includes the SUBJECT DEVICE.

17. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser,

e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

18. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take

substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

19. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain

period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress GUTIERREZ's thumb and/or fingers on the device(s); and (2) hold the device in front of GUTIERREZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

20. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

## VI. CONCLUSION

21. For all of the above reasons, there is probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of July, 2023.

_____
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

PROPERTY TO BE SEARCHED

One red iPhone cell phone, using phone number 562-665-1161, Device ID 891480000072656697 35 (the "SUBJECT DEVICE"), seized on May 2, 2023, from and belonging to the person of Juan Carlos GUTIERREZ and currently maintained in the custody of the Drug Enforcement Administration in Los Angeles, California.

**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (distribution and possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute and possession with intent to distribute controlled substances) (the "SUBJECT OFFENSES") located on the SUBJECT DEVICE, namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from the SUBJECT DEVICE and which relate to the above-named violations;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Houseparty, Facebook,

Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from the SUBJECT DEVICE and which relate to the above-named violations;

d. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs or drug overdoses including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the use, purchase, sale, transportation, or distribution of drugs, or drug overdoses;

f. Contents of any calendar or date book corresponding to the date range of November 9, 2021, to May 2, 2023;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations, between November 9, 2021, and May 2, 2023;

h. Records of or information about the SUBJECT DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that

the user entered into any Internet search engine, and records of user-typed web addresses.

2. The SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

3. With respect to the SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

a. Evidence of who used, owned, or controlled the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software on the SUBJECT DEVICE that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the attachment of other devices to the SUBJECT DEVICE;

d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. Evidence of the times the SUBJECT DEVICE was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the SUBJECT DEVICE, to run software contained on the SUBJECT DEVICE, or to conduct a forensic examination of the SUBJECT DEVICE;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

## II. SEARCH PROCEDURE FOR THE SUBJECT DEVICE

5. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital

device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE(S), the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. During the execution of this search warrant, law enforcement is permitted to (1) depress GUTIERREZ's thumb- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICE (only if the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of GUTIERREZ's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.